UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF FLORIDA

OFFICE OF THE ATTORNEY GENERAL,
STATE OF FLORIDA,
DEPARTMENT OF LEGAL AFFAIRS,

Plaintiff,

v. CASE NO.:

SMARTBIZ TELECOM LLC,
A Florida limited liability company,

Defendant.
_____/

COMPLAINT

Plaintiff, Office of the Attorney General, State of Florida, Department of Legal Affairs ("Attorney General"), by and through the undersigned Assistant Attorneys General, hereby brings this action pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. § 6101 et seq., the Telemarketing Sales Rule, 16 C.F.R. § 310; the Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227 et seq., and Florida's Deceptive and Unfair Trade Practice Act, Chapter 501, Part II, Florida Statutes ("FDUTPA"), against Defendant, Smartbiz Telecom LLC, a Florida limited liability company authorized to transact business in Florida, ("Defendant" or "Smartbiz"). Plaintiff seeks temporary and permanent injunctive relief, the imposition of civil penalties and statutory damages, an award of attorney's fees and costs, and other

legal, statutory, or equitable relief this Honorable Court deems proper, and alleges the following:

INTRODUCTION

1. On any given day millions of American consumers are informed that their "social security number has been found to be involved in illegal activities and will be suspended in the next 24 hours."[1] Others will be told a suspicious iPhone purchase has frozen their Amazon account but that they can press "1" to report it.[2] Sometimes the message can sound relatively benign, like an offer from "Discover" to reduce your credit card interest rate,[3] but regardless of whether the call tries to threaten or entice - it is a scam. At best these calls are annoying, but for many they lead to catastrophic financial losses. Fraudulent robocalls are the most common contact method for scams, and consumers reported losing over $692 million to fraudulent robocalls in 2021 alone.[4]

[1]Defendant transmitted a robocall with this message on February 2, 2021. https://media.youmail.com/mcs/glb/audio/s3diZGlyX2RsaGRmYTp0b21jYXQzMjEyOjE2MTIyOTk3ODI1NThYWza3aJ.gen.mp3

[2] Defendant transmitted a robocall with this message on February 8, 2022. https://media.youmail.com/mcs/glb/audio/s6diZGlyX3J6cWRmYTp0b21jYXQ2Mzc0OjE2NDQzNTc3MTM5OTlSybBRRA.gen.mp3

[3] Defendant transmitted a robocall with this message on January 10, 2022. https://media.youmail.com/mcs/glb/audio/s6diZGlyX2g5amRmYTp0b21jYXQ0NDEyOjE2NDE4MzAyODgzNzhLtRRDkK.gen.mp3

[4] FTC Consumer Sentinel Network Data Book 2021, at 12 (February 2022) https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf

2. Smartbiz is a provider of Voice over Internet Protocol ("VoIP") telephone service.

3. The Industry Traceback Group ("ITG"), a neutral consortium appointed by the Federal Communications Commission ("FCC") to manage private-led efforts to trace back the origin of suspected unlawful robocalls, has notified Smartbiz at least 255 times since April 7, 2020, about fraudulent or otherwise illegal calls that transited Smartbiz's network. According to records produced by the ITG, Smartbiz is one of the most prolific transmitters of illegal robocalls in the United States.

4. Of the approximately 1,225 companies that have received tracebacks,[5] only twenty-eight (28) have received more tracebacks than Smartbiz. That puts Smartbiz in the ninety-eighth percentile for transmitting illegal robocalls. It has been linked to more illegal robocalls than approximately ninety-eight percent (98%) of other companies in its industry.[6] The ITG estimates that each traced call is representative of a large volume of similar illegal calls, meaning Smartbiz has

[5] Registered pursuant to 47 C.F.R. 64.1203, the ITG traces back the most prolific or damaging ongoing illegal robocall campaigns in the United States. This "traceback" process starts when the ITG sends a notice to the "terminating provider," the voice service provider who delivered an illegal robocall to the call recipient. The notice contains a recording or description of the illegal robocall and requests that the terminating provider respond and identify the company which sent it the illegal robocall. The ITG then sends a notification to the company that sent the terminating provider of the illegal robocall and the process repeats until the ITG determines the source of the illegal call or reaches a company that refuses to respond to the traceback notification.

[6] Because tracebacks always begin with the call recipient's voice service provider, companies with large numbers of subscribers appear in more tracebacks than companies, like Smartbiz, that do not provide phone service to consumers directly. Several of the companies that have received more tracebacks than Smartbiz are large cellular carriers.

caused vast numbers of scam robocalls to reach US consumers, despite being told about the problem over and over again.

5. This deluge of scam robocalls invades consumers' privacy and can result in enormous monetary loss to consumers.

6. In turn, Defendant profits from these scam calls. Smartbiz courts robocaller customers by allowing them to place a high volume of calls in quick succession, billing only for the duration of completed calls – sometimes in as little as .6 second increments and ignoring clear indicia of fraudulent call traffic.

7. Smartbiz knows that it carries fraudulent calls. Its contracts contain language that provides the parties shall not withhold any payment on the basis that fraudulent calls comprise a portion of the traffic volume.

8. Despite over 250 tracebacks specifically informing Smartbiz that it is transmitting illegal calls, despite letters from the ITG about Defendant's need to improve its traffic screening procedures, and despite discussions with the Attorney General about steps Smartbiz can take to reduce or eliminate fraudulent calls on its network, Defendant has chosen profit over people and refuses to implement meaningful procedures to prevent perpetration of serious fraud on its network. This lawsuit seeks to hold Smartbiz responsible for its role in flooding the United States with phone scams.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1337(a), 1355; the Telemarketing Act, 15 U.S.C. § 6103(a); and the TCPA, 47 U.S.C. § 227(e)(6) and (g)(2). This Court has pendent jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(1), 1395(a), 47 U.S.C. §§ 227(e)(6)(E), 227(g)(4), and 15 U.S.C. § 6103(e). Defendant resides within this District.

11. Plaintiff has notified the FCC of this civil action as required by 47 U.S.C. §§ 227(e)(6)(B) and (g)(3).

12. Plaintiff has notified the Federal Trade Commission ("FTC") of this civil action as required by 15 U.S.C. § 6103(b).

PLAINTIFF

13. The Attorney General is an enforcing authority of FDUTPA under § 501.203(2), Florida Statutes, and is authorized to bring this action and to seek injunctive and other statutory relief pursuant to §§ 501.207 and 501.2075, Florida Statutes.

14. The Attorney General determined that this enforcement action serves the public interest.

15. The Attorney General is authorized by 15 U.S.C. § 6103(a) of the Telemarketing Act to file actions in federal district court to enjoin violations of, and enforce compliance with, the Telemarketing Sales Rule on behalf of the residents of Florida, and to obtain damages, restitution, or other compensation on behalf of Florida residents.

16. The Attorney General is authorized by 47 U.S.C § 227(e)(6)(A) to bring this action to impose civil penalties.

17. The Attorney General is authorized by 47 U.S.C. § 227(g)(1) to bring this action to enjoin Defendant's illegal calls and for damages.

DEFENDANT

18. Smartbiz is a Florida limited liability company with its principal place of business in Miami, Florida. Smartbiz was organized as a limited liability company effective September 25, 2016.

19. Smartbiz identified itself as a VoIP telecommunications provider, registered in the FCC's Form 499 Filer Database as Filer ID No. 831853.

20. At all relevant times Smartbiz was engaged in trade or commerce within the scope of § 501.203(8), Florida Statutes.

BACKGROUND

Defendant's Business

21. Smartbiz purports to be an intermediate VoIP provider, meaning it accepts calls from upstream VoIP providers, whose call traffic often originates outside the United States, and routes those calls through others, called downstream providers, for delivery to call recipients on the public switched telephone network.[7]

22. Smartbiz structures its contracts and billing to appeal to upstream providers who transmit robocalls.

23. Robocalling technology allows for the transmission of high volumes of calls in a short duration. A robocaller can make multiple calls in a single second. These calls can deliver prerecorded or artificially voiced messages, or they can allow a computer to listen for the call to be answered and then connect the call to a live operator. The hallmark of robocalling is the ability to quickly place high volumes of phone calls in a very short period of time.

24. Robocall technology is particularly attractive to scammers because it allows them to efficiently place millions or billions of calls as they troll for vulnerable consumers who may fall victim to their scams.

[7] The public switched telephone network refers to the aggregate of landline and mobile telephone infrastructure that can be accessed by the public at large. This does not include private communications networks which are only accessible by select individuals such as intercom systems.

25. Smartbiz appeals to upstream providers who transmit robocalls by, *inter alia*, accepting high volumes of very short duration call traffic, billing only for the calls that connect, and billing in extremely short billing increments –as little as .6 seconds. These practices allow robocallers to make huge numbers of call attempts for free and only pay a tiny amount if call recipients immediately hang up, which happens frequently.

26. Smartbiz also appeals to robocallers by allowing calls with obviously false calling phone numbers to transit its network. Robocalls are often made with simulated, or "spoofed," calling phone numbers which allows the caller to deliberately disguise the origin of the call and the caller's actual identity. It is particularly easy to spoof a phone number when making VoIP calls, because the calling phone number is just another piece of data that is transmitted with the call and any string of numbers or letters can be input. Smartbiz does not block calls with invalid or otherwise improper calling phone numbers.

27. For instance, Smartbiz transmits high volume, short duration call traffic that originates in a country that does not use the same numbering format as the United States, but where the calls appear as United States' phone numbers.

28. Telephone numbers used in the United States conform to a numbering convention called the North American Numbering Plan ("NANP"). All NANP numbers allocated to phone service subscribers in the United States follow the

format 1-NXX-NXX-XXXX, where the leading "1" is the country code, N can have a value of 2 through 9, inclusive, and X can have any value 0 through 9, inclusive.

29. Many countries use alternative numbering plans to denote valid telephone numbers. At a minimum, calls from non-NANP numbers will need to display a country code that is different from the country code used by NANP numbers for a caller in the United States to have enough information to return the call.

30. High volume, short duration traffic that originates in non-NANP countries but uses exclusively NANP phone numbers is likely to contain fraudulent calls, as scammers know that potential victims are less likely to answer calls from phone numbers in unfamiliar formats. Moreover, scammers are often not interested in the recipients being able to return their calls, and if the caller's identifying number is spoofed a recipient will not be able to use it as a call back number to reach the scammer.

31. Smartbiz accepts traffic that originates from non-NANP countries but where the calls purport to be from NANP phone numbers, Smartbiz does not require any information from upstream providers to demonstrate that such traffic is legal.

32. Smartbiz accepts upstream VoIP providers' traffic without ever checking whether the purported calling phone numbers appear facially legitimate. For instance, Smartbiz accepts VoIP call traffic where the calling number is invalid

under any country's numbering plan, or where the calling phone number is not a number at all. For instance, Smartbiz connected calls where the caller ID was "USERNAME." This is usually related to some misconfiguration of the caller's robocalling software.

33. More egregiously, Smartbiz also routinely transmits calls from foreign upstream carriers where the purported calling numbers match a US government agency such as the Social Security Administration, a US law enforcement agency such as a local sheriff's office, or a commonly impersonated company such as Bank of America, Apple, Microsoft, or a utility service provider.

34. Smartbiz accepts and connects call traffic which contains calling numbers that purport to be 911. The emergency code 911 is never used for outbound calling. A legitimate call will never display 911 in the caller ID.

Calling Patterns Associated with Illegal Robocalls

35. Even if Smartbiz had not been specifically informed over 250 times that it was carrying fraudulent call traffic, it should have known that it was facilitating scam calls based on the records it maintains.

36. Every attempted call that reaches a VoIP provider's network automatically generates a record which generally includes at least the following information:

a. The date and time of the call attempt;

b. The duration of the call (calls that fail to connect are generally denoted by a zero second duration);

c. The destination or called number of the intended call recipient;

d. The originating or calling number from which the call was placed (which may be a real number or may be spoofed);

e. An identifier such as a name or account number for the upstream provider that sent the call attempt to the VoIP provider's network; and

f. An identifier for the downstream provider to which the VoIP provider attempts to route the call.

37. VoIP providers use these call detail records ("CDRs") for billing purposes and thus have an interest in ensuring that they are complete and accurate.

38. Illegal robocalls create distinctive patterns in CDRs. For instance, these calls are universally unexpected and unwanted and call recipients frequently hang up the phone immediately, so the calls typically connect for a very short duration. CDRs for illegal robocalls will often feature a high percentage of calls that are only a few seconds long, and when examined in the aggregate show a very short average call duration.

39. Conversely, CDRs showing legitimate, consented to robocalls or routine conversational call traffic typically have a much lower percentage of short calls and have a much longer average call duration.

40. Also, Caller ID spoofing is often apparent in CDRs of illegal robocalls.

41. Robocallers use spoofing to both hide their identity and to make it more likely that consumers will answer their calls.

42. One common technique used by illegal robocallers, called neighbor spoofing, is to spoof the calling phone number so it matches the area code and/or the exchange code of the called phone number.[8] This makes it appear to the call recipients that they are getting a local call which they're more likely to answer.

43. Illegal robocallers frequently use caller ID spoofing to impersonate trusted organizations, such as law enforcement, government agencies, and large corporations.

44. Patterns of neighbor spoofing or impersonating trusted numbers are easy to detect when they are present in CDRs and indicate that the upstream provider is sending fraudulent calls across the intermediate provider's network.

45. Another recognizable characteristic of fraudulent robocalls captured by CDRs is the presence of high numbers of unique calling numbers.

46. Robocallers often use a calling number only once or twice to prevent consumers from reporting the phone numbers as associated with scam calls and

[8] In a NANP telephone number the first three digits after the country code of "1," which is often not necessary to dial, are called the area code and correspond to a geographic area. The next three digits are called the exchange code. Historically the exchange code also corresponded to a geographic area; however, this is no longer true.

because many legitimate companies try to block calls from phone numbers that are associated with scams.

47. Legitimate telemarketers and people who make calls for ordinary business or personal purposes use their same phone number for each call they place, and as a result CDRs for legitimate traffic usually show that the total number of calls is significantly greater than the total number of unique phone numbers used. However, CDRs for call traffic that contains fraudulent robocalls generally show that the total number of calls is close to the total number of unique phone numbers. Using a different phone number for each fraudulent robocall is often called "snowshoeing" or using "disposable" phone numbers.

48. Finally, substantial numbers of illegal robocalls are placed to numbers on the National Do Not Call Registry ("DNC List") because fraudulent robocallers are unlikely to respect legal restrictions on calling numbers on the DNC List. High rates of calls to DNC List numbers can distinguish between illegal robocalls and legitimate telemarketing.

49. Defendant has access to CDRs for all of the call traffic that transits its network but does not analyze these CDRs to investigate whether its upstream providers are sending it potentially illegal robocalls.

50. Periodically checking CDRs to better understand and mitigate the problematic traffic it receives from upstream carriers would protect consumers from

scam calls and would ensure that Smartbiz follows the law. Smartbiz knows that it is trafficking in scam calls because, among other reasons, the ITG has informed Smartbiz over 170 times about specific scam calls Smartbiz transmitted. Rather than uncover and cut off illegal call traffic, Smartbiz instead chooses to profit from it.

DEFENDANT KNOWINGLY TRANSMITS ILLEGAL CALLS

Smartbiz is on Notice That it Transmits Illegal Calls

51. Smartbiz receives a traceback notification from the ITG informing it that it is carrying fraudulent call traffic virtually every week. Smartbiz has received at least 255 tracebacks between April 7, 2020, when it received its first traceback, and November 10, 2022. During this 136-week period, Smartbiz received on average approximately 1.8 tracebacks per week.

52. Smartbiz has not gone a month without receiving a traceback since May 2020.

53. This volume and consistency of tracebacks shows that Smartbiz considers transmitting illegal robocalls an acceptable component of its business. The company knowingly continues to transmit these calls despite having the ability to cleanse its network of this traffic.

54. Smartbiz's responses to tracebacks frequently state: "In addition to notified (sic) immediately our customers, they are identified as the account sending us FRAUD calls into the US territory (as we are currently doing). We will require

them to take immediate action and stop these calls while giving information regarding the upstream carrier originating those calls. If we don't receive a formal response and actions taken as requested within 24hrs, Their (sic) account will be blocked temporarily until they comply with our requirements."[9]

55. Smartbiz's traceback history shows that they do not temporarily block upstream providers who send fraudulent call traffic that gives rise to a traceback. For example, in 2022 alone Smartbiz was notified through tracebacks of scam calls they received from the upstream provider Whisl on 3/6, 3/8, 3/30, 4/1, 4/5, 4/26, 5/16, 5/17, 5/19, 5/26, 6/20, 6/21, 6/29, 6/30, 7/14, 7/21, 7/26, 8/3, 8/8, 8/10, 8/11, 8/17, 8/23, 8/24, 8/26, 8/29, 8/30, 9/12, 9/14, 9/21, 10/3, 10/11, 10/15, 10/27 and 10/28. This history indicates that Smartbiz did not block Whisl's traffic at all despite receiving tracebacks repeatedly for calls they received from this customer.

Upstream Provider Call Detail Records

56. On April 21, 2021, pursuant to Section 501.206, Florida Statutes, the Attorney General issued an investigative subpoena to Smartbiz requesting, *inter alia*, CDRs for all call attempts received from four upstream providers who had transmitted calls through Smartbiz that were the subject of tracebacks.

57. SmartBiz provided CDRs for traffic it received from four carriers: OXNP Telecom Limited, AlkaIP Telecom LLC, KWK Communications Inc., and

[9] ITG records noted this response from Smartbiz, verbatim, on several occasions.

Family Communication Pte. Ltd. For each carrier, virtually all of the calls placed by the top twenty calling numbers were associated with scam calls.

58. OXNP's top twenty ANIs[10] accounted for 255,139 calls (15.51%) of the total number of attempted calls by that carrier. Nineteen of those ANIs are associated with scams according to publicly available information on unwanted calls compiled by the companies YouMail and Nomorobo. These ANIs attempted 249,097 calls which were likely fraudulent, including 15,133 calls which used ANIs reported as making scam calls impersonating the Social Security Administration ("SSA").

59. Similarly, publicly available information indicated that seventeen of KWK's top twenty ANIs were associated with scams, fourteen of Family Communication's top twenty ANIs were associated with scams, and all twenty of AlkaIP's top twenty ANI's were associated with scams.

60. The Attorney General's analysis of the top twenty ANIs for each carrier showed that SmartBiz transmitted at least 1,176,889 attempted calls associated with reported scams. In most cases a surface level internet search would show that the ANIs had placed reported scam calls. However, SmartBiz does not perform any such

[10] Calling numbers in CDRs are frequently referred to as "Automatic Number Identifications" or "ANIs." Calling numbers and ANIs are used synonymously unless otherwise stated.

analysis, even though it would likely identify the upstream carriers who are sending fraudulent calls to SmartBiz.

61. Additionally, the Attorney General's analysis of SmartBiz's CDRs showed a high volume of suspicious call traffic featuring calls that spoofed into invalid numbers or numbers associated with the SSA, law enforcement agencies, major corporations such as Apple and Bank of America, and even 911.

62. Traffic transmitted from Family Communications contained at least 6,221 calls using three of Apple's phone numbers.

63. Traffic received from AlkaIP contained calls spoofing Florida law enforcement offices such as the Escambia County Sheriff's Office, as well as federal law enforcement such as the phone numbers for the FBI's Dallas, El Paso, and San Antonio offices.

64. Family and AlkaIP's traffic showed that callers attempted to spoof into 911 for several calls.

65. The Attorney General's analysis of this portion of one day's worth of Smartbiz's call traffic showed at least 10,023 instances where callers attempted to impersonate government offices, corporations, or law enforcement.

Analysis of Full Days of Smartbiz's Call Traffic

66. In order to better understand the composition of SmartBiz's call traffic, the Attorney General issued another investigative subpoena to Smartbiz for all

attempted calls it transmitted into the United States on two days, January 10, 2022 and February 8, 2022, on which the company had transmitted fraudulent calls that were the subject of tracebacks.

67. Smartbiz produced CDRs to the Attorney General which show that many of Smartbiz's upstream provider clients routinely route call traffic to Smartbiz with obvious indicia of fraud.

68. For instance, on January 10, 2022, Smartbiz received 44,290 call attempts from Etelix, a VoIP provider based in Miami, FL that "provides International and Domestic Long-Distance voice termination" to "Long Distance Operators and Long Distance Wholesales (sic) Carriers" among other commercial customers.[11]

69. Most of these calls, 61.7%, were consistent with neighbor spoofing. Both the area code and exchange code of the calling phone number matched the called phone number 43.9% of the time (19,431 calls), and the area code of the called and calling numbers matched 17.8% of the time (7,577 calls). Given that Etelix is a provider of wholesale long-distance phone service, rather than providing service to consumers for local calling, Smartbiz should have been suspicious of this traffic and required Etelix to demonstrate that the traffic is legal or be terminated as a customer.

[11] https://www.etelix.com/ (Last accessed 11-30-2022).

70. Furthermore, of the over 44,000 calls, only seventy-seven (77) had a duration over two (2) minutes and only eighteen (18) lasted longer than fifteen (15) minutes. Also, a different phone number was used for almost every single call – 97% of the phone numbers used appeared only once. Neither of these indications are consistent with local conversational calling or legitimate telemarketing.

71. Finally, the call blocking service YouMail captured a transcription of one of these calls. YouMail's transcription indicates that the call consisted of a prerecorded message which impersonated law enforcement and threatened the recipient with legal action unless they press one to confirm some information.[12]

72. Similarly, Red Telecom, an Egyptian VoIP provider nominally headquartered in Miami, sent Defendant 3,220,367 call attempts over the two days for which the Attorney General subpoenaed records. Only 16,298 (0.51%) of these calls lasted longer than two minutes.

73. Red Telecom's calls featured obvious neighbor spoofing. Approximately 71% of the call attempts made by Red Telecom displayed a calling phone number that matched the area code or both the area code and the exchange code of the called phone number. This pattern is an indication that the calls are

[12] The full transcription of the captured call reads: "There is your priority. So that we can discuss your case and take necessary action on this matter if we don't hear from you then we will be forced to take legal action against you kindly we would like to confirm some information with you before taking legal action. If you want to talk with the administrator please press one I repeat press one thank you."

fraudulent robocalls, particularly in light of the fact that the call traffic was coming from an Egyptian provider but consisted of NANP phone numbers.

74. Again, call content captured by YouMail dispels any doubt that Red Telecom's traffic contained illegal robocalls. Call recordings for these calls included calls fraudulently claiming the recipients' Social Security Number was used improperly[13] and Amazon imposter scam calls,[14] among others.

75. Smartbiz also received call traffic from upstream providers that contained high volumes of short duration calls to numbers on the DNC List.

76. Despite these indicia of fraud, Red Telecom is still Smartbiz's customer and as recently as September 26, 2022, Smartbiz received one of many tracebacks for calls transmitted by Red Telecom.

77. Records Smartbiz provided to the Attorney General for Whisl contained a total of 877,594 call attempts on one day. Of these call attempts, 391,889 resulted in a call with a duration of at least one (1) second. The average duration of connected calls was 11.76 seconds, indicating that these calls were generally not expected or wanted by the recipients.

[13] YouMail transcribed several of these calls which read as follows: "Your social security number is being used for some kind of suspicious activity in the South border of Texas. To know more. Please press one I repeat please press one thank you have a nice day."

[14] YouMail transcriptions of these calls include: "Amount of $1537.35 will be debited from your bank account for the purchases. If you authorize this transaction. No action is required but if you have a dispute with the purchases. Please press one and your call will be connected with Amazon support. I repeat. If you have a dispute. Press one. Thank you."

78. YouMail captured several examples of the calls Whisl transmitted to Smarbiz. These calls included, among others, a call featuring a pre-recorded message that stated "Hello this is Sarah from Discover. I am calling in regards to the rate expiration. We've been trying to reach you as your eligibility for reduction is about to expire. Press one for more information or hang up this call."[15]

79. The call traffic from Whisl included 356,374 call attempts to telephone numbers on the DNC List – 40.61% of the total number of call attempts.

80. The short duration of the calls, the presence of prerecorded messages, and the high volume of calls to numbers on the DNC List, all indicate that most, if not all, of the call traffic from Whisl were fraudulent or otherwise illegal robocalls.

81. Multiple other upstream provider customers of Smartbiz also sent traffic that consists of or includes illegal robocalls and shows obvious indicia of fraud.

COUNT I

Violations of the TCPA – 47 U.S.C. § 227(b)(1)(A)(iii)

82. Plaintiff incorporates and realleges the paragraphs preceding Count I as if fully set forth herein.

[15] A recording of the call is available at: https://media.youmail.com/mcs/glb/audio/s6diZGlyX2g5amRmYTp0b21jYXQ0NDEyOjE2NDE4MzAyODgzNzhLtRRDkK.gen.mp3

83. Section 227(b) of the TCPA, 47 U.S.C. § 227, et seq., prohibits any person within the United States, or any person outside the United States if the recipient is within the United States, from making any call using an automatic telephone dialing system or an artificial or prerecorded voice to any cellular telephone, with exceptions for certain emergency calls or calls placed with the prior express consent of the called party. 47 U.S.C. § 227(b)(1)(A)(iii).

84. The Attorney General is authorized to bring an action for violations of the TCPA when the Attorney General has reason to believe that any person has engaged in a pattern or practice of telephone calls or other transmissions to residents of Florida in violation of the TCPA. 47 U.S.C. § 227(g)(1).

85. Defendant engaged in a pattern or practice of making telephone calls featuring prerecorded or artificially voiced messages to cellular telephone numbers in Florida, and elsewhere, in violation of 47 U.S.C. § 227(b)(1)(A)(iii).

86. CDRs provided by Smartbiz to the Attorney General contain 3,206,193 calls terminated to Florida phone numbers, many of which are cellular telephones. Call recordings captured by YouMail, as well as patterns in the CDRs of these calls, show that many of these calls featured prerecorded or artificially voiced messages.

87. Smartbiz made calls terminated to Florida because the calls would not have connected but for Smartbiz's decision to allow them to transit its network

despite having actual knowledge that many of the calls were scam robocalls featuring prerecorded or artificially voiced messages.

88. Defendant knew or should have known that many of calls it made to Florida violated 47 U.S.C. § 227(b)(1)(A)(iii).

89. Under 47 U.S.C. § 227(g)(1) the Attorney General is entitled to actual monetary loss or $500 in damages for each violation of 47 U.S.C. § 227(b)(1)(A)(iii). Furthermore, because Defendant willfully violated 47 U.S.C. § 227(b)(1)(A)(iii), the amount of such damages may be increased by not more than three (3) times.

COUNT II

Violations of the TCPA – 47 U.S.C. § 227(b)(1)(B)

90. Plaintiff incorporates and realleges the paragraphs preceding Count I as if fully set forth herein.

91. The TCPA prohibits any person within the United States, or any person outside the United States if the recipient is within the united States, from initiating any telephone call to any residential telephone line using an artificial or prerecorded voice to deliver a message without the prior express consent of the called party, unless the call is initiated for emergency purposes, or is exempted by rule or order of the FCC under 47 U.S.C. § 227(b)(1)(B).

92. The Attorney General is authorized to bring an action for violations of the TCPA when the Attorney General has reason to believe that any person has engaged in a pattern or practice of telephone calls or other transmissions to residents of Florida in violation of the TCPA. 47 U.S.C. § 227(g)(1).

93. Defendant engaged in a pattern or practice of initiating telephone calls to residential telephone lines, including telephone lines in Florida, using artificial or prerecorded voices to deliver a message without the prior express consent of the called party in violation of 47 U.S.C. § 227(b)(1)(B).

94. CDRs provided by Smartbiz to the Attorney General contain 3,206,193 calls terminated to Florida phone numbers, many of which are residential telephones. Call recordings captured by YouMail, as well as patterns in the CDRs of these calls, show that many of these calls featured prerecorded or artificially voiced messages.

95. Smartbiz initiated calls terminated to Florida because the calls would not have connected but for Smartbiz's decision to allow them to transit its network despite having actual knowledge that many of the calls were scam robocalls featuring prerecorded or artificially voiced messages.

96. Defendant knew or should have known that many of these calls violated 47 U.S.C. § 227(b)(1)(B).

97. Under 47 U.S.C. § 227(g)(1) the Attorney General is entitled to enjoin violative calls and to actual monetary loss or $500 in damages for each violation of

47 U.S.C. § 227(b)(1)(B). Furthermore, because Defendant willfully violated 47 U.S.C. § 227(b)(1)(B), the amount of such damages may be increased by not more than three (3) times.

COUNT III

Violations of the Truth in Caller ID Act – 47 U.S.C. § 227(e)

98. Plaintiff incorporates and realleges the paragraphs preceding Count I as if fully set forth herein.

99. Under 47 U.S.C. § 227(e)(1), it is unlawful for any person within the United States, or any person outside the United States if the recipient is within the United States, in connection with any voice service or text messaging service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless such transmission is exempted pursuant to FCC regulations.

100. Under 47 U.S.C. § 227(e)(6), the Attorney General may bring a civil action to enforce 47 U.S.C. § 227(e)(1).

101. Defendants violated 47 U.S.C. § 227(e)(1) by knowingly causing the caller identification services of the recipients of their call traffic to transmit misleading or inaccurate caller identification information including spoofed or otherwise misleading and inaccurate phone numbers.

102. Defendant knew or should have known that they transmit and profit from fraudulent robocalls with spoofed or otherwise misleading and inaccurate phone numbers which seek to defraud, cause harm, or wrongfully obtain things of value from the call recipients.

103. Pursuant to 47 U.S.C §§ 227(e)(5)(A) and (e)(6)(A), the Attorney General is entitled to a civil penalty not to exceed $10,000 for each violation of 47 U.S.C. § 227(e)(1), or 3 times that amount for each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $1,000,000 for any single act or failure to act.

COUNT IV

Violations of the Telemarketing Sales Rule, 16 C.F.R. §§ 310.3-310.4

104. Plaintiff incorporates and realleges the paragraphs preceding Count I as if fully set forth herein.

105. Congress directed the FTC to enact rules prohibiting abusive and deceptive telemarketing acts or practices. 15 U.S.C. § 6102(a)(1).

106. The FTC adopted the Telemarketing Sales Rule ("TSR"), 16 C.F.R. §§ 310.1-310.9, pursuant to Congress's grant of rulemaking authority.

107. The TSR prohibits abusive and deceptive acts or practices by "sellers"[16] or "telemarketers"[17] and further prohibits other persons from providing substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any act or practice that violates the TSR.

108. Many of the fraudulent robocalls that transited Smartbiz's network constitute telemarketing and were initially placed by sellers and/or telemarketers within the scope of the TSR.

109. Defendant, on numerous occasions, violated 16 C.F.R. § 310.3(b) by providing substantial assistance or support through its VoIP services to one or more sellers or telemarketers who Defendants knew, or consciously avoided knowing, were engaged in abusive and deceptive telemarketing acts or practices that violated the TSR.

110. Defendant routinely assisted and facilitated fraudulent robocalls which:

a. Violated 16 C.F.R. § 310.3(a)(2)(iii) by misrepresenting material aspects of goods or services;

[16] 16 C.F.R. § 310.2(dd) defines "seller" as "any person who, in connection with a telemarketing transaction, provides, offers to provide, or arranges for others to provide goods or services to the customer in exchange for consideration."

[17] 16 C.F.R. § 310.2(gg) defines "telemarketing," in relevant part, as "a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call." 16 C.F.R. § 310.2(ff) defines "telemarketer" as "any person who, in connection with telemarketing, initiates or receives telephone calls to or from a customer or donor."

b. Violated 16 C.F.R. § 310.3(a)(2)(vii) by misrepresenting the seller or telemarketer's affiliation with corporations or government entities;

c. Violated 16 C.F.R. § 310.3(a)(4) by making false or misleading statements to induce any person to pay for goods or services;

d. Violated 16 C.F.R. § 310.4(a)(8) by failing to transmit or causing to be transmitted the telephone number and the name of the telemarketer to caller identification services used by call recipients;

e. Violated 16 C.F.R. § 310.4(b)(1)(iii)(B) by calling telephone numbers on the DNC List; and

f. Violated 16 C.F.R. § 310.4(d)(1) by failing to disclose the identity of the seller.

111. Under 15 U.S.C. § 6103(a), the Attorney General is entitled to enjoin Defendant's violations of the TSR and obtain damages and restitution on behalf of those injured by the fraudulent robocalls Defendant transmitted.

COUNT V

Violations of Chapter 501, Part II, Florida Statutes

112. Plaintiff incorporates and realleges the paragraphs preceding Count I as if fully set forth herein.

113. FDUTPA states that "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."

114. The provisions of FDUTPA are to be construed liberally to promote the protection of the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices. § 501.202, Florida Statutes.

115. FDUTPA defines a "violation of this part" to include violations of the Act based on "[a]ny rules promulgated pursuant to the Federal Trade Commission Act" or "[a]ny law, statute, rule, regulation, or ordinance which proscribes unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices." § 501.203(3), Florida Statutes.

116. "A violation of the TSR constitutes an unfair and deceptive act or practice in violation of § 5(a) of the FTC Act." *United States v. Dish Network, L.L.C.*, 75 F. Supp. 3d 942, 1004 (C.D. Ill. 2014).

117. The TSR's enabling statute is the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 USC §§ 6101-08).

118. Under 15 U.S.C. § 6102(c)(1) violations of the TSR are treated as violations of rules passed under the Federal Trade Commission Act (15 U.S.C. § 57a).

119. Violations of rules passed under the FTC Act are unfair and deceptive within the scope of 15 U.S.C. § 45. 15 U.S.C. § 57a(d)(3).

120. Defendant's violations of the TSR are per se violations of FDUTPA.

121. Defendant's conduct also violates FDUTPA because knowingly transmitting fraudulent robocalls to consumers in Florida and elsewhere is a deceptive trade practice.

122. Defendant routinely transmits calls to consumers which misrepresent the identity of the caller and the nature of goods and services offered through the calls.

123. Particularly when the caller's phone number has been spoofed, consumers acting reasonably in the circumstances would be deceived to their detriment when receiving many of the calls transmitted by Defendant.

124. Furthermore, the call traffic Defendant transmits causes injury, or the risk of injury, to consumers which is substantial, one that consumers cannot reasonably avoid, and is without offsetting benefits to consumers or competition.

125. Defendant's practices complained of herein are unfair or deceptive or both and constitute violations of § 501.204, Florida Statutes; therefore, Defendant is liable for injunctive, and other equitable, legal, or statutory relief.

126. Defendant is also liable for civil penalties, as prescribed by Sections 501.2075 and 501.2077, Florida Statutes for each unfair act or practice it willfully engaged in, as set forth above, found to be in violation of FDUTPA.

127. Finally, Defendant is also subject to attorney's fees and costs pursuant to Section 501.2075, Florida Statutes.

PRAYER FOR RELIEF

WHEREFORE, the Attorney General requests that this Honorable Court:

A. Enter judgment in favor of Plaintiff and against the Defendant for the violations as alleged herein;

B. Temporarily and permanently enjoin Defendant from transmitting fraudulent robocalls to consumers in Florida and elsewhere in the United States;

C. Award the Attorney General damages of not more than $1,500 per violation of 47 U.S.C. § 227(b)(1)(A)(iii);

D. Award the Attorney General damages of not more than $1,500 per violation of 47 U.S.C. § 227(b)(1)(B);

E. Award the Attorney General a civil penalty not to exceed $10,000 for each violation of 47 U.S.C. § 227(e)(1), or 3 times that amount for each day of a continuing violation;

F. Temporarily and permanently enjoin Defendant from transmitting calls which violate the TCPA, TSR, or FDUTPA as complained of herein;

G. Award restitution for consumers injured by the fraudulent robocalls Defendant transmitted;

H. Award civil penalties, attorney's fees, and costs against Defendant pursuant to Sections 501.2075 and 501.2077, Florida Statutes, or as otherwise authorized by law;

I. Grant such other legal or equitable relief as this Honorable Court deems just and proper.

Dated: December 5, 2022.

Respectfully Submitted,

ASHLEY MOODY
Attorney General of the State of Florida

/s/ Patrick Crotty
Patrick Crotty
Florida Bar # 108541
Senior Assistant Attorney General
Office of the Attorney General
Consumer Protection Division
3507 E. Frontage Road, Suite 325
Tampa, FL 33607
Phone: 813-287-7950
Fax: 813-281-5515
Patrick.Crotty@myfloridalegal.com

Sarah Cortvriend
Florida Bar # 718947
West Palm Beach Bureau Chief
Office of the Attorney General
Consumer Protection Division
1515 North Flagler Drive, Suite 900
West Palm Beach, FL 33401
Tel: (561) 837-5007

Fax: (561) 837-5109
sarah.cortvriend@myfloridalegal.com

Miles Vaughn
Florida Bar # 1032235
Assistant Attorney General
Office of the Attorney General
Consumer Protection Division
3507 E. Frontage Road, Suite 325
Tampa, FL 33607
Phone: 813-287-7950
Fax: 813-281-5515
Miles.vaughn@myfloridalegal.com